RISE IN RANSOMWARE ATTACKS PUSHES

state leaders to develop smarter backup and recovery strategies

StateScoop Report

Security experts point to modern and affordable platforms that can discover, back up and recover data at scale, and provide significantly greater safeguards against attackers.

There have been at least 270 reported *ransomware attacks* targeting public sector agencies during the past three years, and the pace of attacks show no signs of letting up. In fact, a survey by StateScoop found that more than 8 in 10 federal, state and local government IT officials believe ransomware will be as great a threat — or a greater threat — in the coming year.

The evidence to date suggests their concerns are well placed. In May 2019, a ransomware attack struck the city of Baltimore, encrypting thousands of city government computers. The attackers demanded a ransom of 13 bitcoins — a little more than $100,000 at the time — in exchange for the decryption keys. But city officials have since set aside *$10 million for recovery costs*. Similar incidents have occurred in Florida, Georgia, New York, Ohio and elsewhere across the country.

According to a *StateScoop survey*, underwritten by Veritas, 1 in 3 state government IT leaders reported their state agency had been impacted by ransomware over the past three years. While half of respondents said their agencies have procedures in place to recover or isolate data in the event of a ransomware/malware attack, the study found agencies may not be as prepared as officials think.

Ransomware developers have gotten smarter when it comes to targeting state and local governments. They know, for example, that many lack the resources and expertise to develop sophisticated guidelines for disaster recovery and continuity of operations that could facilitate the restoration of data.

Federal officials and cybersecurity experts also warn of increasing ransomware campaigns from state-sponsored actors. The U.S. Treasury, for instance, said *North Korean-backed hacking groups* have escalated the use of ransomware attacks on critical infrastructure to fund the regime's missile programs. And a top Department of Homeland Security official, Christopher Krebs, recently recommended government agencies "pay close attention to your critical systems," mindful of *potential retaliation* by Iran's state-sponsored hackers following the U.S.'s killing of the country's top military general.

If state government officials are intent on avoiding the disruption and expense of a ransomware attack, they need to make sure they have the necessary backup and recovery platforms in place to effectively separate and protect their data from would-be attackers, say security experts.

"I think officials are still in a bit of denial around the impact and the preponderance of ransomware," said Rick Bryant, National Healthcare Architect and Ransomware Expert at Veritas Technologies. "Ransomware developers quickly realized that they needed to hide their tracks and they needed to be able to make sure that the agencies couldn't back up. As a result, a lot of the modern-day ransomware attacks actually look for backup workloads and encrypt those first, before unleashing their payloads into the operating environment."

Discover, backup, recover — at scale

Understanding the dangers of modern ransomware is essential to realizing the importance of modernizing data protection and backup and recovery capabilities.

There are two kinds of ransomware encryption. One type will have keys that are required to decrypt the data being held for a ransom. With the other kind of encryption used, there are no keys. What makes this type of encryption particularly malicious is that a random key generator is used to generate unique keys for each file and no digital record is kept of the keys. Even if a ransom is paid, the data cannot be decrypted. The data is left essentially inaccessible with no way to decrypt the files, requiring a complete restore from backup.

Given the evolution of ransomware, there are inherent advantages to adopting systems like Veritas' *NetBackup* (recognized by *Gartner* for 14 years running), as well as Veritas Resiliency Platform and *APTARE IT Analytics* tools to help agencies achieve greater resiliency. These capabilities have been engineered specifically to protect against unexpected losses in citizen services and employee productivity in a way that future-proofs the investment.

Data discovery

Putting defenses in place against ransomware is only one piece of the puzzle. It is critical for agencies to capture data management insights as a means to develop a comprehensive data protection strategy.

According to Bryant, the first step toward building that strategy is to discover what data your agency has and where it lives. "Knowing what's important, where it's located, and who has access to it is paramount to being able to effectively protect it," he said.

> The first step toward building a comprehensive data protection strategy is … knowing what data is important, where it's located, and who has access to it.
>
> **– Rick Bryant, Veritas Technologies**

WHERE LOSS OF DATA FROM RANSOMWARE POSES GREATEST RISKS FOR STATE AGENCIES

Percent of state IT executives who said:

53%

Unbudgeted expenses for remediation

49%

Prolonged productivity loss

47%

Employee productivity loss

46%

Loss of institutional trust

43%

Substantial program damage requiring reconstruction of department records

8%

Risk to national security

Source: ***StateScoop Survey***

17%

said their agencies could recover fully within 12 hours from a ransomware/ malware attack

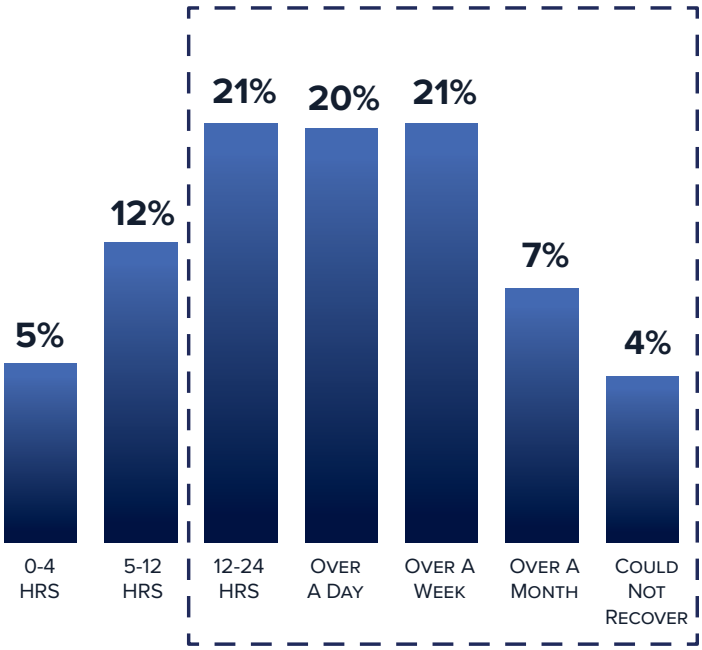
RANSOMWARE HAS DIRECTLY AFFECTED

32%

of State IT respondents in the past 3 years

AGENCIES FACE LENGTHY RECOVERY DELAYS

State Respondents



Q: If your most critical data was affected by a ransomware/ malware attack, how long would it take your department to fully recover without paying the ransom?

Source: ***StateScoop survey***

Through its Information Studio, Veritas is able to provide visibility, targeted analysis and informed action on data to identify areas of waste, risk and value. With the power to organize data and take informed action, organizations can be confidently prepared to handle security concerns, new regulations and continuous data growth.

“Our Information Studio or Insights products have the ability to actually collect metadata about all of the files that exist within a company’s organization,” said Mike Malaret, Veritas Technology’s Director of Sales Engineering for the Defense and Intelligence Communities. “So if we can detect anomalies within the environment and remediate them prior to actually worrying about them getting caught in the backup site, we’re in a much better place,” he said.

“The Insights technology component is very important for being able to add that extra layer of security, give agencies insights into the data that shouldn’t be there and, therefore, deleted, and also help give them insights on where their

critical data actually exists," Bryant said. "Our Predictive Insights components can actually help you proactively scan your environment for malware or ransomware types of extensions to eliminate it before it activates."

Bryant recommends agencies take steps to appropriately tier their data based on the relative value of that data. "If data hasn't been accessed in six months, move it to a lower tier, a lower accessibility level or delete it," he said. "Maybe even move it to the cloud, but understand where it is and manage the cost associated with it. Just putting everything in a file share that everybody has access to is foolhardy and rife with problems."

Secure your backup

Because ransomware attacks are increasingly targeting backups, the best approach is to deploy backup appliances that protect the backup workload itself. And the best practice that Malaret suggests is multiple copies of data backed up in multiple locations.

An agency's choice of backup solution is also critical to its ability to restore a large scale environment in a reasonable amount of time in the wake of a ransomware attack. "That's where that backup becomes critical," Malaret said.

"If you use a Veritas appliance, it has data center security and application whitelisting, meaning that the ransomware can't get into it, but also anything the attackers come up with tomorrow can't get into it unless it's specifically programmed to allow an interaction or communication," Bryant said. "If you build it yourself, you still need to put in good safeguards to protect those backup workloads or you can just use our purpose-built appliance," he said. "We can literally recover thousands of systems at the same time."

Investing in better backup controls can also help agencies future-proof their ransomware protections. "They can use it today to protect on-prem workloads. And if later they get a backup data center, it will work in that environment as well," Bryant said. "It can even back up to the cloud."

Recover at scale

Data recovery scenarios can be extremely complex for public agencies. And at the state and local level, agencies are measured by how quickly they can recover from a ransomware incident. However, budget pressures continue to be a challenge. Forty-two percent of agencies cite lack of budget as a major obstacle to their efforts to defend against ransomware, according to the StateScoop survey.

> So if we can detect anomalies within the environment and remediate them prior to actually worrying about them getting caught in the backup site, agencies are in a much better place.
>
> **– Rick Bryant, Veritas Technologies**

"They either don't have the backups or they don't have the funds to be able to recover," Bryant said. "It makes it even more critical that state and local agencies have preparations in place to protect, prevent and then rapidly recover because they're not going to be able to get extra money."

The Baltimore attack in May 2019 – which has cost the city upwards of $10 million in recovery – made clear that state and local agencies may find themselves financing a more modern and effective backup and recovery system, whether they want to or not. Doing so with a strategic plan to get there now would be preferable to having to do so after an event.

And that speaks to Veritas' unique value proposition, according to Bryant. "We can help them by protecting those backup workloads, we can help them recover at scale and we can help them address their number one concern, which is budget overruns," he said.

Learn more about how Veritas Technologies can safeguard your agency's data from the perils of ransomware attacks.

This StateScoop report was produced for, and sponsored by, Veritas Technologies.

statescoop VERITAS™